Notes (03/06/2024)

The video discusses various types of hackers and their roles in the digital landscape:

1. **White Hat Hackers:** Ethical guardians who use their hacking skills for good, exposing vulnerabilities and strengthening defenses to protect data and privacy.
2. **Gray Hat Hackers:** Operate in the middle ground between ethical white hats and malicious black hats. They expose vulnerabilities without permission, potentially offering solutions for a fee, with questionable legality and ethics.
3. **Red Hat Hackers:** Act as activists or vigilantes, operating outside the law to fight against cybercriminals and organizations they deem unethical, using aggressive tactics.
4. **Black Hat Hackers:** Nefarious hackers with malicious intent, violating laws and ethical boundaries for personal gain, vengeance, or chaos, causing financial losses, privacy breaches, and disruptions.
5. **Script Kiddies:** Individuals with limited technical knowledge who use pre-written scripts and software to exploit known vulnerabilities, often causing harm without understanding the consequences.
6. **Activists:** Individuals using hacking skills for political or social activism, engaging in digital civil disobedience to raise awareness or challenge authorities.
7. **Nation State Hackers:** Individuals or groups working for a government to conduct cyber attacks for national interests, posing a significant threat due to their skills and state backing.
8. **Whistleblowers:** Expose wrongdoings for the public interest, protected by laws, but contrasted with malicious insiders who exploit their access for personal gain or harm.
9. **Cyber Terrorists:** Individuals or groups using the internet to launch attacks causing violence, disruption, or fear to advance political or ideological agendas.
10. **Gaming Hackers:** Exploit vulnerabilities in video games to gain unfair advantages, risking account bans and legal repercussions.
11. **Cryptojackers:** Cybercriminals hijack devices to secretly mine cryptocurrency, draining resources without the user's knowledge.
12. **Bot Masters:** Masterminds behind botnets, networks of compromised computers used for various malicious purposes.
13. **Social Engineers:** Manipulate human psychology rather than technical vulnerabilities to gain access or information.
14. **Phishers:** Deceptive individuals posing as trusted entities to trick victims into revealing sensitive information.
15. **Spammers:** Unsolicited messages aiming to spread malware, trick individuals, or waste time.
16. **Crackers:** Malicious burglars breaking into digital spaces with the intent to steal data, disrupt operations, or wreak havoc.

17. **Zero Day Exploit Specialists:** Individuals who specialize in exploiting newly discovered software vulnerabilities before they are known, with controversial but crucial knowledge.
18. **Advanced Persistent Threat:** Sophisticated cyber attacks backed by nation states targeting high-value organizations for extended periods, posing a major threat.
19. **Black Markets for Hackers:** Hidden online markets where hackers trade illegal goods, services, and stolen data.
20. **Malware Developers:** Crafters of malicious software with various motivations, fueling cybercrime and requiring a multi-pronged approach for mitigation.
21. **Blue Hat Hackers:** Ethical security professionals working independently to find and report vulnerabilities in systems.
22. **State-Sponsored Hackers:** Backed by governments, these hackers conduct cyber attacks to advance national interests.
23. **Activist Collectives:** Groups using cyber attacks to promote social or political causes, often employing various tactics to raise awareness or disrupt operations.

Also view at https://sites.google.com/view/owca/notes/03-06-2024